

GEMMA Gegevenslandschap

Logging van verwerking van gegevens

Leeswijzer

Dit document beschrijft de visie van VNG Realisatie ten aanzien van de opslag en ontsluiting van de metagegevens van verwerkingen van gegevens. Dit document behoort tot de architectuurdocumenten van de ontwikkeling van de gemeentelijke informatievoorziening: het GEMMA Gegevenslandschap. In deze visie worden de gemeentelijke bewegingen op het gebied van de informatievoorziening geschetst, en wordt aan de hand van deze bewegingen een nieuwe, flexibele en meer generieke en gezamenlijke gemeentelijke informatievoorziening geschetst.

Dit document is bestemd voor informatiemanagers, adviseurs, architecten en productmanagers van gemeenten en gemeentelijke leveranciers.

Het document is als volgt opgebouwd:

- Hoofdstuk 1 beschrijft de inleiding;
- Hoofdstuk 2 beschrijft het vigerende beleid en kaders;
- Hoofdstuk 3 beschrijft de huidige- en toekomstige gemeentelijke informatiearchitectuur;
- Hoofdstuk 4 beschrijft de scope van logging van verwerkingen en eisen die eraan gesteld worden;
- Hoofdstuk 5 de mogelijke inrichtingsvarianten voor de opslag van de logging;
- Hoofdstuk 6 beschrijft de gemeentelijk inrichting;
- Hoofdstuk 7 beschrijft de NLX (Common Ground) implementatie van logging;
- Hoofdstuk 8 beschrijft de samenhang met componenten uit de GEMMA.

Dit document is in beheer bij VNG-Realisatie.

Versie	Toelichting	Datum	Opsteller(s)
1.0	Eerste vastgestelde versie	november 2018	VNG Realisatie
1.1	Aanpassingen n.a.v. consultatie met gemeenten en leveranciers	oktober 2019	VNG Realisatie

Inhoudsopgave

Leeswijzer.....	2
Inhoudsopgave	3
1. Inleiding	5
2. Beleid en kaders.....	6
2.1. Visie Nederlands kabinet.....	6
2.2. Europees Kader: Algemene Verordening Gegevensbescherming (AVG).....	7
2.2.1. Rechtmatige verwerking (verwerkingsgrondslag en doelbinding).....	8
2.2.2. Dataminimalisatie.....	8
2.2.3. Juistheid van persoonsgegevens.....	8
2.2.4. Opslagbeperking (bewaartermijnen).....	8
2.2.5. Beveiliging van persoonsgegevens.....	9
2.2.6. Specifieke aanvullende verplichtingen uit de AVG.....	9
2.3. Nationaal kader: Uitvoeringswet AVG (UAVG).....	11
2.3.1. Regeling van het BSN in de Uitvoeringswet AVG.....	11
3. Informatiearchitectuur.....	13
3.1. Huidige inrichting	13
3.2. Toekomstige inrichting.....	14
3.3. Uitgangspunten voor huidige en toekomstige situatie	16
3.4. Het register in de informatiearchitectuur.....	17
4. Scope van, en eisen aan logging van verwerkingen.....	18
4.1. Scope.....	18
4.2. Eisen aan logging	18
5. Inrichtingsvarianten	20
5.1. Centrale inrichting.....	22
5.2. Gefedereerde inrichting	25
6. Gemeentelijke inrichting	28
6.1. Opslag van loggegevens	29
6.2. Ontsluiting van logging.....	30
6.3. Filtering van loggegevens.....	31
7. NLX implementatie logging.....	32

7.1. Architectuur.....	32
7.2. Opslag loggegevens	33
7.3. Ontsluiting van logging.....	34
8. GEMMA componenten	35
8.1. Loggingregister	36
8.2. Logginginzagecomponent.....	36
Bijlage 1: Bronnen	37

1. Inleiding

Een van de belangrijke doelen van het kabinet is het versterken van de weerbaarheid van burgers en organisaties. In de visie Nederland Digitaal en de Digitale Agenda Overheid is verwoord op welke manier hieraan invulling wordt gegeven. Een belangrijk begrip hierbij is verantwoording naar de burger kunnen afleggen over welke persoonsgegevens, voor welk doel en door wie zijn verwerkt. Dergelijke transparantie vergroot het inzicht van de burger en daarmee het vertrouwen van de burger in de overheid.

In de visie van de overheid wordt aan de burger wordt via mijnOverheid in de toekomst inzage gegeven in de gegevens die door de overheid en haar keten- en netwerkpartijen verwerkt zijn in het kader van de uitvoering van de publieke taak.

“Om het vertrouwen in systemen te vergroten, hebben mensen het recht op inzicht wie, op welk moment en voor welk doel, hun gegevens inziet, gebruikt of aan anderen geeft. Dit recht is vastgelegd in de Algemene Verordening Gegevensbescherming. Dit vraagt veel van alle overheidsorganisaties en mogelijk leidt dit tot gezamenlijke acties.”

Bron: NL DIGIbeter - Agenda Digitale Overheid, juli 2018

Het bieden van transparantie naar burgers over de verwerking van (persoons)gegevens heeft gevolgen voor de inrichting van de informatiesystemen van gemeenten. Verwerkingen van (persoons)gegevens, zowel binnen de gemeente als met keten- en netwerkpartijen, moeten vastgelegd worden en deze verwerkingen moeten aan de burger inzichtelijk gemaakt kunnen worden. De huidige gemeentelijke informatiesystemen kunnen maar zeer beperkt voldoen aan deze eisen. Om te borgen dat in de (nabije) toekomst gemeenten invulling kunnen geven aan de gestelde eisen is het van belang om de bijhouding en ontsluiting van verwerkingen (logging) te standaardiseren binnen de gemeentelijke informatiearchitectuur.

In deze notitie wordt beschreven op welke wijze gemeenten gebeurtenissen met betrekking tot de activiteiten van gebruikers en systemen (verwerkingen) kunnen vastleggen in audit-logbestanden en wordt beschreven hoe vanuit deze logbestanden transparantie ten aanzien van het handelen van de gemeente naar burger, ondernemer en bestuurder kan worden afgeleid.

Daar waar in deze notitie wordt gesproken over de gemeente mag ook worden gelezen gemeentelijke samenwerkingsverband of SaaS dienstverlener voor een gemeente.

2. Beleid en kaders

2.1. Visie Nederlands kabinet

Digitalisering transformeert wereldwijd economieën en maatschappijen in een razendsnel tempo. Nederland heeft een goede uitgangspositie om de economische en maatschappelijke kansen van digitalisering te verzilveren. De digitale infrastructuur is van wereldklasse, de beroepsbevolking is goed opgeleid en we hebben een traditie van samenwerking, bijvoorbeeld tussen bedrijfsleven, kennisinstellingen en overheid. Tegelijkertijd roept digitalisering ook nieuwe, fundamentele vragen op. Bijvoorbeeld over de bescherming van onze privacy en de toekomst van onze banen. Om de kansen van digitalisering te benutten en antwoorden te geven op deze vragen moet Nederland voorop lopen met digitalisering. Met onderzoek, experimenten, het toepassen van nieuwe technologie en constructieve discussies over ethische vraagstukken. Op die manier versterken we het Nederlands verdienvermogen, kunnen we beter richting geven aan technologische ontwikkelingen en zetten we vol in op de economische en maatschappelijke kansen van digitalisering. Om voorop te kunnen lopen moeten we ook het vertrouwen van burgers en bedrijven vergroten. Daarom versterken we het fundament – o.a. privacybescherming, cybersecurity, digitale vaardigheden en eerlijke concurrentie - voor digitalisering. De uitdaging bij deze transformatie is om iedereen binnen boord te krijgen én te houden. Op de arbeidsmarkt, maar ook in de samenleving als geheel.

Het kabinet zet daarom in op een aanpak met twee sporen:

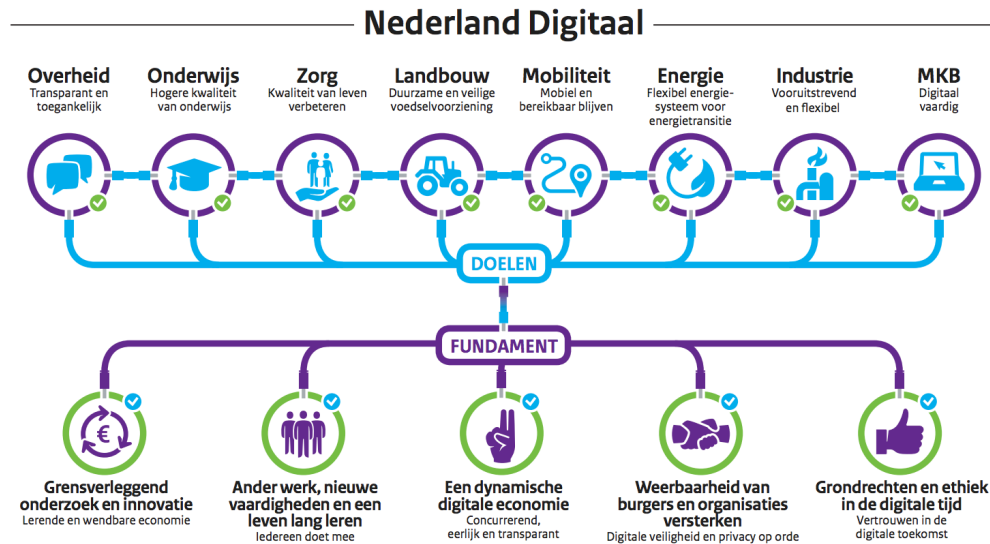
1. Maatschappelijke en economische kansen benutten (versnellen)
Digitalisering vindt voor een belangrijk deel plaats in maatschappelijke sectoren waar de overheid een relatief grote rol heeft. Denk aan de zorg, mobiliteit, energie en het agrifood-domein. Ook de verdere digitalisering van het openbaar bestuur zelf is een belangrijke opgave. De uitdaging voor het kabinet is om in deze sectoren de digitale transitie te versnellen en te ondersteunen.
2. Het fundament voor digitalisering – waaronder privacybescherming, cybersecurity, digitale vaardigheden en eerlijke concurrentie – moet op orde zijn en verder worden versterkt. Het kabinet zet hiervoor in op vijf speerpunten, zodat burgers en bedrijven de kansen kunnen benutten die digitalisering biedt.

Het fundament van Nederland Digitaal is nader uitgewerkt in 'NL DIGIbeter', de Agenda Digitale Overheid van alle overheden gezamenlijk, die in juli 2018 is vastgesteld door de Ministerraad. Deze agenda legt verbinding met publieke en private partners om kansen en vraagstukken van de digitalisering door de overheid op te pakken. Door NL DIGIbeter heen staan de behoeften en rechten van burgers en ondernemers centraal. De Agenda biedt enerzijds ruimte om op een innovatieve manier te werken aan maatschappelijke vraagstukken. Aan de andere kant wordt voortgebouwd op de bestaande voorzieningen om de dienstverlening beter en persoonlijker te maken. Bijvoorbeeld door modernisering van de overheidsportalen zodat mensen op één plek zaken met de overheid kunnen regelen die aan hun persoon gekoppeld is.

Verder besteedt de Agenda veel aandacht aan zowel grondrechten en publieke waarden (bijvoorbeeld bij datagebruik) als ook de toegankelijkheid/begrijpelijkheid van digitale dienstverlening (inclusie). Dat betekent dat mensen het recht hebben op digitale dienstverlening, maar ook dat voor inwoners die niet digitaal geholpen kunnen of willen worden er andere vormen van contact mogelijk is.

VNG Realisatie

Nassaulaan 12 Den Haag | Postbus 30435, 2500 GK Den Haag
070 373 8008 | realisatie@vng.nl



Figuur 1 - Nederland Digitaal

Belangrijk onderdeel van NL DIGIbeter is het persoonlijker maken van de dienstverlening, bijvoorbeeld door de inwoner meer inzage en regie te geven op de eigen gegevens. Gemeenten spelen dan ook een grote rol bij de sturing op voorzieningen van de digitale basisinfrastructuur die juist betrekking hebben op die dienstverlening. Denk hierbij aan mijnOverheid en identiteitsmiddelen.

Het onderwerp van dit document, het vastleggen van verwerkingen van persoonsgegevens en de ontsluiting van deze vastlegging maakt deel uit van het fundament van Nederland Digitaal. Binnen het onderdeel "Weerbaarheid van burgers en organisaties versterken" is vanuit het beschermen van de persoonsgegevens en de rechten van burgers aandacht voor het feit dat de eigen regie van burgers op persoonsgegevens moet worden vergroot om daarmee de bescherming van privacy verder te bevorderen. Een van de beoogde resultaten op dit vlak is dat mensen er op moeten kunnen vertrouwen dat zij laagdrempelig en veilig inzage kunnen krijgen in hun persoonsgegevens **en het gebruik daarvan door derden**, én dat ze deze gegevens (waar mogelijk) kunnen corrigeren, verwijderen en (her)gebruiken.

2.2. Europees Kader: Algemene Verordening Gegevensbescherming (AVG)

De AVG is sinds 25 mei 2018 rechtstreeks van toepassing. Met de Uitvoeringswet Algemene verordening gegevensbescherming (zie voor een toelichting hierna) is de Wet bescherming persoonsgegevens (Wbp) ingetrokken. De AVG hanteert voor de bescherming van persoonsgegevens een bepaalde systematiek om op basis van een aantal privacy beginselen te komen tot afgewogen keuzes voor de bescherming van persoonsgegevens. Daarnaast schrijft de AVG aanvullend op een aantal aspecten meer in detail voor hoe persoonsgegevens moeten worden beschermd. In dit kader zijn het meest van belang de "transparantierechten" die aan betrokken worden toegekend en de verplichtingen om privacy by design als uitgangspunt te nemen en een PIA uit te voeren om zicht te krijgen op feitelijk spelende privacy risico's en daarop maatregelen te treffen. De kern van de AVG wordt gevormd door een aantal grondslagen en beginselen dat als uitgangspunt moet worden genomen bij de (inrichting van) verwerking van persoonsgegevens. Deze grondslagen en beginselen worden hieronder toegelicht.

2.2.1. Rechtmatige verwerking (verwerkingsgrondslag en doelbinding)

Uit de AVG volgt in de eerste plaats dat de verzameling en verwerking van persoonsgegevens plaatsvindt op een rechtmatige en behoorlijke wijze (artikel 5, eerste lid, aanhef en onder a, van de AVG). Verder dienen de doeleinden waarvoor verzameling en verwerking plaatsvindt gerechtvaardigd, welbepaald en uitdrukkelijk omschreven te zijn (doelbinding). Voor overheidsorganisaties geldt daarbij dat zij voor de verwerking van persoonsgegevens voor de hen toegekende taken het kader van die taken over een expliciete verwerkingsgrondslag moeten beschikken.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Bij de vastlegging van verwerkingen dienen de doeleinden en verwerkingsgrondslagen waarvoor verzameling en verwerking plaats hebben gevonden te worden geregistreerd zodat verantwoording, zowel naar de burger als naar het bestuur, afgelegd kan worden over de rechtmatigheid van de verwerkingen.

2.2.2. Dataminimalisatie

Persoonsgegevens die worden verwerkt moeten toereikend en ter zake dienend zijn, en beperkt zijn tot wat noodzakelijk is voor de doeleinden. Daarbij gaat het om proportionaliteit en subsidiariteit, waardoor een minimum aan verwerking van persoonsgegevens wordt gerealiseerd (artikel 5, eerste lid, onder c, van de AVG). Er mogen niet meer gegevens dan nodig worden verwerkt en er moet goed worden gezien of het doel niet op een manier kan worden bereikt die minder inbreuk maakt op privacy.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Bij de vastlegging van verwerkingen dient vastgelegd te worden welke gegevens, of categorieën van gegevens tijdens de verwerking zijn gebruikt. Door deze vastlegging kan verantwoording worden afgelegd over proportionaliteit en subsidiariteit van het verwerkende proces. Bij de vastlegging van de verwerking worden geen inhoudelijke gegevens opgeslagen buiten een identificerend attribuut waarmee de verwerking aan een persoon of ander object kan worden gerelateerd. Deze vastlegging is nodig om bij een verzoek om inzage de verwerkingen te kunnen koppelen aan de juiste persoon.

2.2.3. Juistheid van persoonsgegevens

De AVG bepaalt ook dat moet worden voorzien in maatregelen om te zorgen dat persoonsgegevens op een juiste wijze worden verwerkt en dat maatregelen worden getroffen om te zorgen dat gegevens die niet (meer) juist worden verwerkt, gerectificeerd of verwijderd worden (artikel 5, eerste lid, onder d, van de AVG).

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Voor wat betreft de vastlegging van verwerkingen heeft deze eis geen directe doorwerking. Het is de verantwoordelijkheid van de processen die gegevens verwerken om invulling te geven aan maatregelen die de juistheid van gegevens borgen.

2.2.4. Opslagbeperking (bewaartermijnen)

Een volgend belangrijk uitgangspunt is dat persoonsgegevens niet langer worden verwerkt dan voor een termijn die gelet op het doel van verwerkingen noodzakelijk en daarmee te rechtvaardigen is (artikel 5 eerste lid, onder f, van de AVG).

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Het moet mogelijk zijn om gegevens van verwerkingen die niet langer bewaard hoeven te worden te verwijderen. De bewaartermijn van gegevens is afhankelijk van de verwerkende processen. Bij de vastlegging van de verwerkingen dient aangegeven te worden wat de bewaartermijn vanuit het verwerkende proces is zodat de termijn ook gehanteerd kan worden voor de vastgelegde gegevens over de verwerkingen (de logging).

2.2.5. Beveiliging van persoonsgegevens

Bij de verwerking van persoonsgegevens moeten technische en organisatorische maatregelen worden getroffen, zodanig dat een passende beveiliging gewaarborgd is (artikel 5, eerste lid, onder f, van de AVG). Ten aanzien van de beveiliging van persoonsgegevens werkt artikel 32 van de AVG dit uit. Bepaald wordt dat, waar passend, pseudonimisering en versleuteling dienen te worden ingezet. NB: pseudonimisering is dus niet per definitie verplicht, maar kan als oplossing behulpzaam zijn bij problemen ten aanzien van herleidbaarheid en het voorkomen van kwetsbare gegevensconcentraties. Ook wordt aangegeven dat maatregelen moeten worden genomen om te zorgen dat op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen kan worden gegarandeerd, en dat de beveiligingsmaatregelen op gezette tijden getest en geëvalueerd worden. Voorts volgt uit dit artikel dat dient te worden voorzien in maatregelen om, bij een fysiek of technisch incident, de beschikbaarheid van en de toegang tot persoonsgegevens tijdig te kunnen herstellen. Voor de inrichting van beveiliging van persoonsgegevens dient rekening te worden gehouden met de zogeheten Richtsnoeren beveiliging Persoonsgegevens, waarin de AP de wijze waarop beveiliging van persoonsgegevens kan plaatsvinden nader heeft uitgewerkt¹.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Aan burgers moet inzage gegevens kunnen worden in de persoonsgegevens die door de gemeente verwerkt zijn. Om deze transparantie te kunnen bieden is het vereist om de vastgelegde verwerkingen te kunnen koppelen aan de burger. Voorkomen moet worden dat de vastlegging van verwerkingen leidt tot een kwetsbare gegevensconcentratie. Denk bijvoorbeeld aan het vastleggen van een onversleutelde BSN in de logging. Dit zou kunnen leiden tot een privacy hotspot doordat verwerkingen over verschillende organisaties en processen via het BSN aan elkaar gekoppeld kunnen worden. Uitgangspunt is daarom dat dergelijke gegevens gepseudonimiseerd worden alvorens de verwerking wordt vastgelegd in de logging.

2.2.6. Specifieke aanvullende verplichtingen uit de AVG

Naast de modellering van bescherming van persoonsgegevens aan de hand van deze beginselen, regelt de AVG ter ondersteuning en kadering daarvan ook nog aan aantal meer concrete verplichtingen. De in dit kader meest relevante verplichtingen worden hieronder besproken.

Inregelen faciliteiten voor uitoefening rechten betrokkenen

Transparantie voor betrokkenen heeft in de AVG een belangrijke plaats gekregen. Een van de kernprincipes in de AVG is dat burgers zicht en controle kunnen houden over hun persoonsgegevens en kunnen ingrijpen als dat nodig is (hoofdstuk 3 AVG). De AVG kent aan burgers rechten tot om controle te houden over hun gegevens. Veel rechten zoals het inzage- en correctierecht, golden al onder de Wbp, maar een aantal rechten

¹ <http://wetten.overheid.nl/BWBR0033572/2013-03-01>

is nieuw of meer in de aandacht gezet, zoals het “vergeetrecht (op verzoek wissen van gegevens)” en het recht op overdraagbaarheid van gegevens (“dataportabiliteit”).

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Het vergeetrecht is ten aanzien van de vastgelegde verwerkingen beperkt van toepassing. In de logging worden naast een gepseudonimiseerde identiteit geen persoonsgegevens vastgelegd. Het recht op dataportabiliteit is niet van toepassing aangezien het gaat om de vastlegging van daadwerkelijk uitgevoerde verwerkingen door een specifieke organisatie. Dergelijke gegevens zijn niet overdraagbaar naar een andere organisatie.

Privacy by design (& by default)

De AVG verplicht expliciet om in het ontwerp (design) van systemen en standaardinstellingen (default) reeds van het begin af aan rekening te houden met bescherming van persoonsgegevens. Er dienen bij het ontwerp technische en organisatorische maatregelen te zijn getroffen die de gegevensverwerking strikt beperken tot de noodzaak en persoonsgegevens mogen in beginsel – systeemtechnisch, d.w.z. zonder bewuste keuze - niet verwerkt/gedeeld worden.

Privacy by design komt er kortgezegd op neer dat bij de inrichting en inregeling van systemen en processen die de noodzakelijke verwerkingen van persoonsgegevens ondersteunen rekening wordt gehouden met de bescherming van persoonsgegevens. In feite betreft dat een weerslag van afweging tussen de genoemde privacy beginselen een invulling van de wijze waarop aan transparantieplichtingen kan worden voldaan.

Privacy by default komt er op neer dat bij oplevering van een nieuwe voorziening standaard alles dicht staat en voor het openstellen van bijv. toegang expliciet actie nodig is.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Door geen inhoudelijke (persoons)gegevens vast te leggen maar alleen meta-gegevens over een verwerking wordt de gegevensverwerking beperkt tot de strikt noodzakelijke gegevens. Als technische maatregel wordt pseudonimisering toegepast om te voorkomen dat identificerende gegevens van burgers misbruikt kunnen worden.

Data protection impact assessment (DPIA)

Uiteindelijk gaat het bij de bescherming van persoonsgegevens om het voorkomen van privacy risico's en (vooral ook) om het voorkomen van onwenselijke gevolgen ervan voor burgers.

Naar aanleiding van de motie-Franken heeft het kabinet bepaald dat bij de ontwikkeling van beleid en wetgeving waaruit gegevensverwerkingen voortvloeien, bij de bouw van ICT-systemen en de aanleg van grote databestanden een DPIA moet worden uitgevoerd. De AVG verplicht tot het voorafgaand uitvoeren van een DPIA voor gegevensverwerkingen met een hoog risico voor de rechten en vrijheden van natuurlijke personen. Daarvan wordt in elk geval geacht sprake te zijn als er sprake is van verwerkingen van persoonsgegevens met een hoog risico, zoals bij de inzet van nieuwe technieken of grootschalige gegevensverwerking - voorafgaand daarop – een DPIA uit te voeren. Doel er van is om – aanvullend op de inrichting van bescherming van persoonsgegevens op grond van de reeds besproken beginselen, scherper zicht te krijgen op de feitelijk bij de

verwerking of in de context spelende privacy risico's en daarmee – als correctiemechanisme - rekening te houden bij de uiteindelijke (ontwerp) en beveiligingsmaatregelen.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Het uitvoeren van een DPIA op een voorgestelde inrichting van de vastlegging van logging van de gemeentelijke informatiesystemen lijkt gezien de verwerking van het BSN in de logging noodzakelijk te zijn².

Sluitstuk AVG: register- en verantwoordingsplicht

De AVG vereist dat organisaties (zowel verantwoordelijken als verwerkers) aantoonbare controle hebben over de persoonsgegevens die zij verwerken. Dit betekent dat een register moet worden bijhouden van alle verwerkingen van persoonsgegevens die plaatsvinden. De AVG schrijft concreet voor welke gegevens ten aanzien van verwerkingen moeten worden bijgehouden. Ook moet actief aandacht worden besteed aan, en maatregelen geïmplementeerd waaruit blijkt dat de organisatie de AVG-beginselen voor verwerking van persoonsgegevens naleeft.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Gemeenten zijn verplicht een register van verwerkingen te voeren. Informatiesystemen die een verwerking van persoonsgegevens uitvoeren dienen deze verwerking te relateren aan een doelbinding en grondslag uit het gemeentelijk register. In de vastlegging van de verwerking van gegevens door gemeentelijke informatiesystemen worden de doelbinding en grondslag als meta-gegevens bij de verwerking vastgelegd.

2.3. Nationaal kader: Uitvoeringswet AVG (UAVG)

Met de UAVG wordt uitvoering gegeven aan de AVG. De AVG is een Europese verordening. Dat betekent dat voor de lidstaten nog maar beperkt ruimte is voor de nationale wetgever om op het terrein van de verwerking van persoonsgegevens zelf iets (afwijkends) te regelen. Daar waar de verordening nog wel ruimte laat voor nationale keuzes, is gekozen om zo dicht mogelijk te blijven bij de Wbp (beleid-neutrale implementatie). In dit verband is het meest relevant dat artikel 87 van de AVG een grondslag geeft om bij nationaal recht specifieke voorwaarden te stellen voor de verwerking van nationale identificatienummers, in Nederland onder meer het BSN.

2.3.1. Regeling van het BSN in de Uitvoeringswet AVG

De Uitvoeringswet AVG regelt het gebruik van wettelijk voorgeschreven nummers, beleidsneutraal en overeenkomend met het voorheen geldende artikel 24 van de Wbp. De nu geldende regels voor verwerking van het BSN worden dus gecontinueerd. Dit betekent dat voor verwerking van het BSN een wettelijke grondslag nodig is. Voor overheidsorganen betreft artikel 10 van de Wabb. Voor de verwerking van het BSN

² Zie: <https://www.informatiebeveiligingsdienst.nl/nieuws/checklist-data-privacy-impact-analyse/>

door private partijen betekent de regeling dat dient te worden voorzien in een specifieke wettelijke grondslag. Hieronder wordt dit nader toegelicht.

Artikel 46 van de UAVG regelt dat een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, bij de verwerking van persoonsgegevens slechts gebruikt wordt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. In feite is dit een kapstokbepaling, op basis waarvan in andere wetten invulling kan worden gegeven aan dergelijke nummers.

In de praktijk bestaat soms de wens het BSN ook voor andere doelen te gebruiken dan ter uitvoering van de wet waarin het voorschrift over het nummer is opgenomen. Dit is alleen gerechtvaardigd als aan twee vereisten is voldaan. Ten eerste geldt het algemene vereiste dat persoonsgegevens alleen verder mogen worden verwerkt als dat verenigbaar is met de doeleinden waarvoor ze zijn verkregen. Ten tweede bepaalt artikel 46 van de Uitvoeringswet dat verwerking van persoonsnummers voor andere doeleinden dan de uitvoering van de betreffende wet alleen mogelijk is voor zover dat bij de wet is bepaald. Dit is een aanvullende eis op die van verenigbaarheid omdat het gebruik van persoonsnummers extra risico's met zich kan brengen voor de bescherming van de persoonlijke levenssfeer, zoals bijvoorbeeld identiteitsfraude.

Eventuele andere gebruiksdoelen dienen derhalve door de formele wetgever zelf te worden vastgesteld. Er komt ten aanzien van de verdere verwerking van het BSN geen eigen afweging toe aan de verwerkingsverantwoordelijke. Hiermee is in de Uitvoeringswet gebruik gemaakt van de nationale ruimte die de verordening biedt om specifieke voorwaarden te stellen aan de verwerking van een nationaal identificatienummer op grond van artikel 6, tweede lid, en 87 van de verordening.

Doorwerking voor de vastlegging- en ontsluiting van verwerkingen van gegevens:

Het BSN mag door gemeenten worden gebruikt als dat noodzakelijk is voor de goede vervulling van hun publiekrechtelijke taak. De Wet algemene bepalingen burgerservicenummer (Wabb) biedt deze wettelijke grondslag voor gemeenten. Bij het loggen van verwerkingen van die vanuit de publieke taak worden uitgevoerd is het derhalve toegestaan om het BSN, het liefst gepseudonimiseerd, op te slaan. Voor de privaatrechtelijke taken van een gemeente ligt dat anders³. Voor het gebruik van het BSN in dat kader is geen wettelijke grondslag. Het gebruik van het BSN is binnen de processen van de bedrijfsvoering derhalve niet rechtmatig.

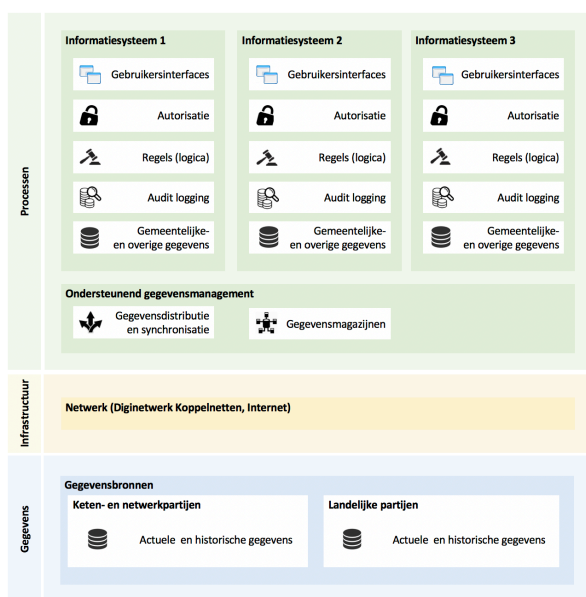
De verplichting om de burger inzage te geven in de verwerking van persoonsgegevens geldt voor zowel publiek- als privaatrechtelijke verwerkingen. Bij het loggen van verwerkingen die voortvloeien uit de privaatrechtelijke taken van een gemeente dient een ander identificerend attribuut gebruikt te worden dan het BSN.

³ <https://autoriteitpersoonsgegevens.nl/nl/nieuws/gebruik-bsn-de-bedrijfsvoering-van-de-overheid>

3. Informatiearchitectuur

3.1. Huidige inrichting

Gemeenten maken voor de uitvoering van hun taken gebruik van een groot aantal gegevensverwerkende informatiesystemen. Deze informatiesystemen zijn veelal gericht op de ondersteuning van een specifiek gemeentelijk domein. Voorbeelden van dergelijke domeinen zijn sociale zaken, belastingen en burgerzaken. Daarnaast wordt door gemeenten gebruik gemaakt van informatiesystemen die een meer horizontale taak hebben. Voorbeelden hiervan zijn documentsystemen en gegevensmagazijnen. Al deze informatiesystemen worden zowel qua functionaliteit als gebruikte gegevens door leveranciers afgebakend. Daar waar mogelijk wordt door leveranciers gebruik gemaakt van nationale- en internationale standaarden, bijvoorbeeld op het gebied van gegevensmodellering (denk aan het Suwi-Gegevensregister⁴ en INSPIRE⁵). De informatiesystemen bieden zelfstandig gebruikersinterfaces, autorisatie, bedrijfsregels, logging en gegevensopslag.



Figuur 2 - Gemeentelijke informatiesilo's

⁴ <https://www.bkwi.nl/producten/suwinet-services/suwinet-standaarden/suwi-gegevensregister-sgr>

⁵ <https://www.geonovum.nl/onderwerpen/inspire>

De informatiesystemen werken als informatiesilo's. Gegevens die worden verwerkt uit basisregistraties worden binnen de silo's en via synchronisatie- en distributiemechanismen synchroon gehouden met de oorspronkelijke bron.

In de huidige situatie waarin gemeenten de applicaties van (veel) verschillende leveranciers gebruiken die elk op hun eigen manier de gegevensverwerking vormgeven is het voor de gemeente een complexe uitdaging volledig compliant te zijn met de AVG. Informatiesystemen zijn meestal niet ingericht op de eisen die vanuit de AVG gesteld worden. Principes zoals het kennen en vastleggen van een 'doelbinding' als grond voor een verwerking worden binnengemeentelijk slechts in uitzonderingsgevallen geïmplementeerd. Het is hierdoor voor gemeenten in de praktijk onmogelijk om de verwerking van persoonsgegevens in- en extern op een adequate manier te verantwoorden. De opzet en complexiteit van het gemeentelijk applicatielandschap biedt ook niet de verwachting dat op korte termijn volledig aan de eisen vanuit de AVG voldaan kan worden.

De Wet Digitale Overheid (invoering naar verwachting eind 2018) verplicht gemeenten een sluitende audit trail van informatietransacties tussen gebruikers en de gemeente bij te houden. Het bijhouden van de complete audit-trail van een informatietransactie vraagt om een samenhangende gestandaardiseerde inrichting van de gemeentelijke informatiearchitectuur op het gebied van het gebruik van doelbinding en grondslagen en de vastlegging van verwerkingen van (persoons)gegevens. De huidige applicaties van gemeenten dienen aangepast te worden aan deze eis.

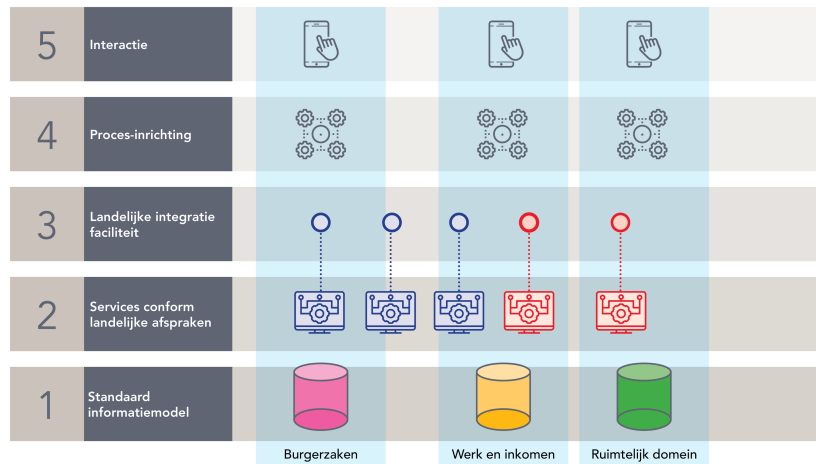
3.2. Toekomstige inrichting

Gemeenten moeten groeien naar een situatie waarin burgers eenvoudig kunnen worden gefaciliteerd in hun rechten. Daarnaast moet de gemeente op eenvoudige, en liefst geautomatiseerde wijze, inzage kunnen geven welke medewerker of rol, op welk moment toegang heeft gehad tot persoonsgegevens of deze heeft bewerkt. Per gemeentelijk proces moet worden bepaald welke functionaliteiten moeten worden ondersteund en voor wie (rol). Door gemeenten is hiervoor een nieuwe inrichting van gemeentelijke informatiesystemen geschetst binnen de Common Ground beweging⁶. Kern van deze beweging is het scheiden van processen en gegevens en het bevragen van gegevens bij de bron. Door de Common Ground beweging is een vijf-lagenmodel geïntroduceerd waarmee verantwoordelijkheden logisch, en ook fysiek van elkaar gescheiden kunnen worden in:

- interactie met eindgebruikers,
- inrichting van processen,
- integratiefunctie
- ontsluiting van gegevens via diensten, en
- gestandaardiseerde opslag van gegevens.

Het grote voordeel van de inrichting van informatiesystemen volgens dit model is dat het niet alleen goedkoper is, maar ook meer ruimte biedt om sneller en gemakkelijker te innoveren. Het Common Ground model maakt tevens gemeenten minder afhankelijk van hun vaste leveranciers en geeft burgers en ondernemers meer en beter inzicht in de wijze waarop met hun gegevens wordt omgegaan.

⁶ <https://vng.nl/samen-organiseren/common-ground>



Figuur 3 - Common Ground vijf-lagen model

Door VNG Realisatie is het Common Ground vijf-lagenmodel nader uitgewerkt naar functionaliteiten die door de verschillende lagen moeten, of kunnen, worden geboden. Deze nadere uitwerking, ook wel *het GEMMA Gegevenslandschap* genoemd schetst de informatiearchitectuur voor de informatiesystemen en gegevensbronnen van de toekomst.

Uitgangspunt binnen het gemeentelijk gegevenslandschap is dat alle verwerkingen van gegevens worden uitgevoerd conform vastgestelde doelbinding en grondslagen, en worden gelogd voor auditing en verantwoordingsdoeleinden. Onderdeel van het gemeentelijk gegevenslandschap is, conform vereisten vanuit de AVG, een register waarin wordt bijgehouden welke verwerkingen van persoonsgegevens plaatsvinden binnen de gemeenten en met welke grondslag dit gebeurt. Vanuit het GEMMA Gegevenslandschap wordt aan informatiesystemen de verplichting opgelegd dat verwerkingen door informatiesystemen gerelateerd zijn aan de in het verwerkingenregister opgenomen verwerkingen. Tevens wordt de verplichting opgelegd om deze verwerkingen vanuit informatiesystemen te loggen en de relevante onderdelen van de logging open te stellen naar burgers.

Applicaties die volgens de uitgangspunten van het GEMMA Gegevenslandschap worden ontwikkeld zijn hierdoor compliant aan de wet- en regelgeving op het gebied van privacy en bescherming van de persoonsgegevens.

3.3. Uitgangspunten voor huidige en toekomstige situatie

Gemeenten beschikken nu over informatiesystemen die op het gebied van de bescherming van de privacy vrijwel nooit voldoen aan de eisen die vanuit wetgeving gesteld worden. De huidige informatiesystemen dienen hierop aangepast te worden, en tegelijkertijd worden gemeenten geconfronteerd met een nieuwe denkwijze ten aanzien van de manier waarop de informatiesystemen ingericht moeten worden (scheiding van processen van gegevens). Hierdoor zal in de komende jaren een mix ontstaan van informatiesystemen die gebaseerd zijn op de huidige en toekomstige inrichtingsprincipes.

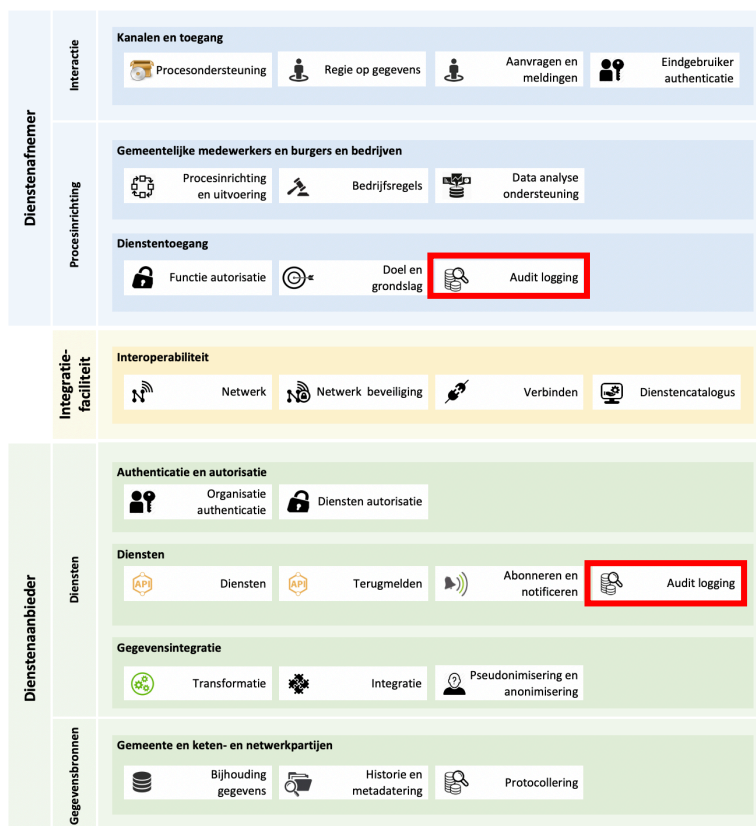
Ten aanzien van de vastlegging en ontsluiting van verwerkingen worden de volgende uitgangspunten gehanteerd:

- De gemeente voert een register van verwerkingen waarin wordt vastgelegd welke (persoons)gegevens door de gemeente worden verwerkt, met welke doelbinding en welke grondslag. Dit register bevat minimaal de doelbindingen en grondslagen van de verwerkingen van persoonsgegevens maar is niet gelimiteerd tot slechts persoonsgegevens;
- Verwerkingen binnen een informatiesysteem worden gerelateerd aan de combinatie van een doelbinding en een grondslag uit het verwerkingenregister;
- De metagegevens van verwerkingen van gegevens door een informatiesysteem worden vastlegt in een logregistratie;
- De logregistratie dient als bron voor verantwoording van het handelen van de gemeente richting burger en bestuur;
- Loggegevens uit de logregistratie kunnen voor een bepaalde tijd verborgen worden voor afnemers om te voorkomen dat burgers en ondernemers voortijdig op de hoogte worden gebracht van (fraude) onderzoeken;
- Zowel voor het register van verwerkingen als voor de logregistratie worden standaard informatiemodellen en APIs gedefinieerd. Deze informatiemodellen en APIs dienen door informatiesystemen, zowel bestaande als nieuwe, geïmplementeerd te worden voor de vastlegging en ontsluiting van loggegevens.

De bovenstaande uitgangspunten doen recht aan de binnen wet- en regelgeving gestelde eisen en gelden voor alle informatiesystemen die (persoons)gegevens verwerken, zowel informatiesystemen die op de huidige- als de nieuwe inrichtingsprincipes zijn gebaseerd. Door in de manier van het loggen van verwerkingen en het hanteren van doelbinding en grondslagen geen onderscheid te maken in informatiesystemen die gebaseerd zijn op de 'oude' of 'nieuwe' inrichtingsprincipes wordt het voor gemeenten mogelijk om voor de verantwoording van verwerkingen gebruik te maken van één bron, ongeacht het type informatiesysteem.

3.4. Het register in de informatiearchitectuur

Door VNG Realisatie is de gewenste informatiearchitectuur beschreven in het ‘*GEMMA Gegevenslandschap*’⁷. Onderdeel van het gemeentelijk gegevenslandschap is, conform vereisten vanuit de AVG, de bijhouding van audit-logging. Vanuit het GEMMA Gegevenslandschap wordt aan informatiesystemen de verplichting opgelegd dat verwerkingen door informatiesystemen inclusief een doel en een wettelijke grondslag worden vastgelegd in een logregister. Tevens wordt de verplichting opgelegd om deze logging open te stellen naar geautoriseerde afnemers.



Figuur 4 - GEMMA Gegevenslandschap

In bovenstaand figuur is weergegeven dat het onderdeel “Audit logging” zich zowel bevindt in de procesinrichtinglaag van dienstenafnemers als in de dienstenlaag van dienstenaanbieders. Hiermee wordt duidelijk gemaakt dat het de verantwoordelijkheid van de zowel de afnemer als de leverancier van een dienst is om verwerkingen te loggen.

⁷ https://www.gemmaonline.nl/index.php/Thema_Samen_organiseren

4. Scope van, en eisen aan logging van verwerkingen

4.1. Scope

Logging door informatiesystemen is grofweg op te delen in een tweetal verschillende soorten logging

- Automatische logging zoals 'technische logging' en 'audit logging'.
- Handmatige logging zoals logboeken van beheerders over uitgevoerde werkzaamheden, bijvoorbeeld: het starten van de back-up of het wisselen van de back-up tapes.

In de "*Aanwijzing logging*"⁸ van de Informatiebeveiligingsdienst (IBD) worden deze verschillende vormen van logging uitgebreid beschreven. De scope van dit document beperkt zich uitsluitend tot audit logging. Het document beschrijft de inrichting van de vastlegging in audit-logbestanden van gebeurtenissen met betrekking tot de activiteiten van gebruikers en systemen (verwerkingen⁹). Voor verwerkingen van persoonsgegevens is logging verplicht, voor de verwerking van overige objecten is deze optioneel.

4.2. Eisen aan logging

Aan de gegevens die ten aanzien van verwerkingen worden vastgelegd worden een aantal eisen gesteld. Deze eisen liggen op het gebied van de vertrouwelijkheid, integriteit, actualiteit, volledigheid en rechtmatigheid.

Actualiteit

Het is de verantwoordelijkheid van zowel een dienstenaanbieder als een dienstenafnemer om te borgen dat het logregister actueel is. Dit betekent dat bij een verwerking de (meta)gegevens van de verwerking direct vastgelegd dienen te worden. Indien een verwerking niet kan worden gelogd dan mag de verwerking ook niet worden uitgevoerd.

⁸ <https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>

⁹ EU-AVG, Art.4: "verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Volledigheid

Het is de verantwoordelijkheid van zowel een dienstenaanbieder als een dienstenafnemer om de verwerking van gegevens te loggen. In het geval van CRUD-verwerkingen zal in veel gevallen slechts één object bij een verwerking betrokken zijn. Het is echter mogelijk dat binnen een API de gegevens van meerdere objecten worden verwerkt. Denk hierbij bijvoorbeeld aan een dienst die op basis van een zoekopdracht gegevens van meerdere objecten (bv personen) retourneert. Om te borgen dat per object inzicht kan worden gegeven in de verwerkingen dient voor ieder object waarvan gegevens verwerkt binnen een proces of dienst een apart logrecord aangemaakt te worden.

Bij de uitvoering van de publieke taak worden door gemeenten (persoons)gegevens uitgewisseld met keten- en netwerkpartijen. Deze uitwisselingen dienen als verwerking vastgelegd te worden. Voorzieningen dienen getroffen te worden om te borgen dat een audit trail van de verwerkingen bij de gemeente kan worden samengesteld.

Integriteit

De logregistratie dient als bron voor de verantwoording van de rechtmatigheid van verwerkingen door de gemeente. De inhoud van de logregistratie dient boven alle twijfel verheven te zijn. Logbestanden dienen derhalve immutable (onaanpasbaar) te zijn. Op geen enkele wijze mag het mogelijk zijn om de logbestanden aan te passen worden na het aanmaken van een logrecord zonder dat dit zichtbaar is. Een eventuele correctie dient in de vorm van een nieuw record te worden toegevoegd zodat eenmaal aangemaakt records nooit gewijzigd worden. Zowel technische als organisatorische maatregelen dienen getroffen te worden om dit te borgen.

Privacy

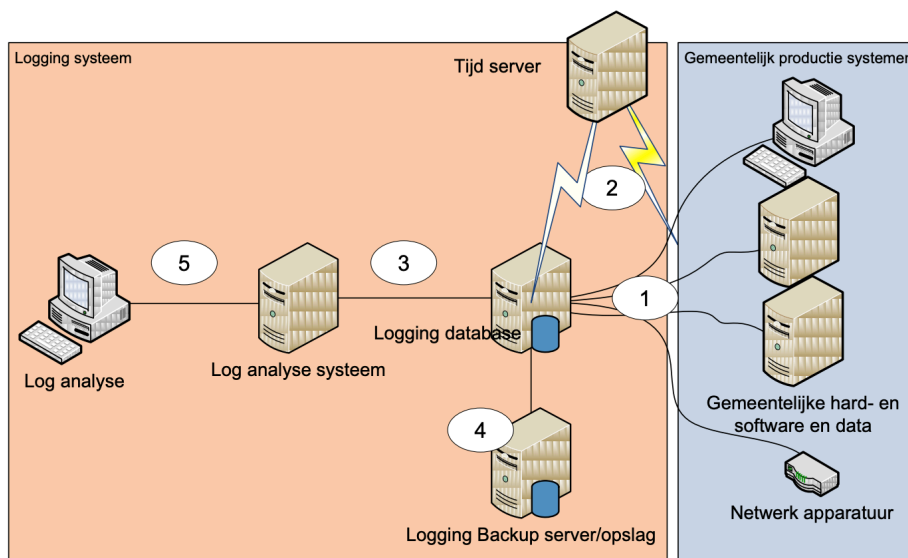
Er moet worden voorkomen dat het logregister privacy risico's introduceert. Het moet worden voorkomen dat een logregister een privacy hotspot kan worden van waaruit een profiel van een burger opgesteld kan worden. Eventuele identificerende eigenschappen van persoonsgegevens dienen gepseudonimiseerd te worden alvorens in de logregistratie opgenomen te worden. Het gebruik van pseudoniemen voorkomt dat de gegevens uit het logregister direct kan worden gerelateerd aan een persoon.

Rechtmatigheid

Het logregister wordt door de gemeente gebruikt om zowel naar burgers en ondernemers als naar het bestuur de rechtmatigheid van verwerkingen van gegevens mee aan te tonen. Om aan te tonen dat een verwerking rechtmatig is geweest is het onder andere van belang dat bekend is wie de verwerking heeft uitgevoerd en vanuit welke doelbinding en grondslag deze persoon de verwerking heeft uitgevoerd. Al de informatie die vereist is voor het kunnen afleggen van verantwoording en het bieden van transparantie dienen in het logregister opgenomen te worden.

5. Inrichtingsvarianten

Informatiesystemen die (persoons)gegevens verwerken dienen metagegevens ten aanzien van deze verwerkingen te loggen. De logging dient ter verantwoording van het handelen van de gemeente richting het bestuur en de burger of ondernemer. Onderstaand figuur geeft weer hoe een logging opzet er globaal uit ziet.



Figuur 5 - Globale inrichting logging¹⁰

1. Logging wordt vanuit de systemen naar een centrale logging database gezonden.
2. Alle systemen hebben dezelfde tijd en gebruiken een tijd synchronisatie bron.
3. De logging database wordt benaderd vanuit een loganalyse systeem.
4. Logging die langere tijd ongebruikt blijft wordt apart gezet in een back-up server.
5. Het loganalyse systeem wordt gebruikt door loganalyse werkstations.

¹⁰ Bron: Logging aanwijzing gemeentelijke informatiebeveiligingsdienst.
<https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>

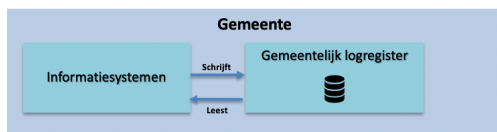
Voor de opslag en ontsluiting van de metagegevens van een verwerking in een logging database (hierna: logregister) zijn een aantal inrichtingsvarianten te onderkennen:

1. Inrichting als centrale voorziening

Metagegevens van verwerkingen worden door gemeentelijke informatiesystemen opgeslagen in een gemeentelijk logregister. Dit register kan vanuit een centrale voorziening worden gefaciliteerd, maar het kan ook lokaal binnen één gemeente als centrale voorziening voor die gemeente worden ingericht. Een centrale voorziening biedt APIs voor aanmaken en ontsluiten van loggegevens;



Figuur 6 - Inrichting van logregistratie als centrale landelijke voorziening



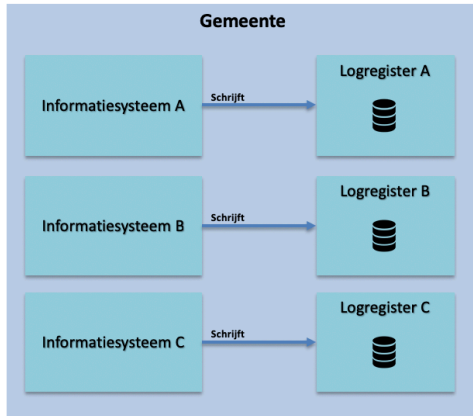
Figuur 7 - Inrichting van logregistratie als centrale gemeentelijke voorziening

2. Inrichting als gefedereerde voorziening

Op het moment dat de loggegevens niet in een centrale registratie worden opgeslagen spreken we van een gefedereerde inrichting. Een gefedereerde inrichting kan op zowel landelijk en gemeentelijk niveau.

- Bij een landelijke gefedereerde inrichting is iedere gemeente verantwoordelijk voor het bijhouden van de loggegevens van de organisatie.

- Bij een lokale gefedereerde inrichting is ieder informatiesysteem binnen de gemeente verantwoordelijk voor de bijhouding van logging in een eigen logregistratie. Bij een lokale gefedereerde inrichting zijn er dus vele voorkomens van een logregistratie binnen de gemeente.



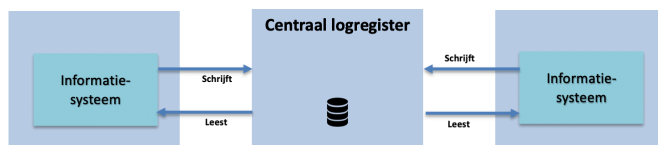
Figuur 8 - Inrichting van logregistratie als lokale gefedereerde voorziening

Beide vormen van inrichting, zowel centraal als gefedereerd, kennen belangrijke voor- en nadelen. Deze worden in de onderstaande paragrafen beschreven.

5.1. Centrale inrichting

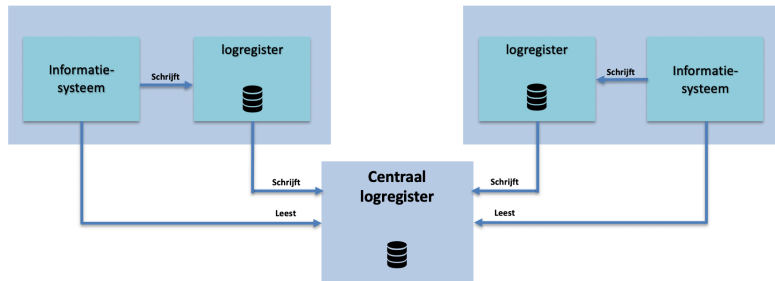
In een scenario waarin logging centraal is ingericht sturen de informatiesystemen van gemeenten hun loggegevens naar een centrale voorziening. Deze voorziening kan lokaal bij de gemeente zijn ingericht als centrale gemeentelijke voorziening, collectief als gemeentelijke voorziening of landelijk als landelijke voorziening. Afnemers kunnen, mits geautoriseerd, de in het logregister opgeslagen gegevens inzien.

Ongeacht de vorm (gemeentelijk individueel, gemeentelijk collectief of landelijk) kan een centrale voorziening worden geïmplementeerd als een bronregistratie of als een magazijn. In het geval van een bronregistratie worden de loggegevens enkel in het centrale register opgeslagen, de aanleverende informatiesystemen houden deze gegevens lokaal niet bij. Er ontstaat hierdoor gemeentelijk, collectief of landelijk een 'single point of truth' ten aanzien van de opslag van metagegevens van verwerkingen.



Figuur 9 - Inrichting van een centraal logregister als bronregistratie

Een andere optie is om de centrale voorziening in te richten als magazijn. In dit geval houden informatiesystemen zelf de metagegevens van verwerkingen in een lokale logregistratie bij en sturen zij deze door naar de centrale logregistratie. De centrale opslag bevat in deze constructie een afslag (redundante kopie) van de loggegevens van informatiesystemen.



Figuur 10 - Inrichting van een centraal logregister als magazijn

Generiek gelden een aantal generieke voor- en nadelen van een centrale inrichting van de logregistratie ongeacht of het een centrale, collectieve of lokale inrichting betreft. Voordelen van een centrale inrichting als bronregistratie is dat er een 'single-point-of-thruth' ontstaat op het niveau waar de voorziening is ingericht. Er hoeft niet gesynchroniseerd te worden met bronhouders, de gegevens worden maar één maal opgeslagen. Een specifiek nadeel van een centrale inrichting als bronregistratie is dat er een single-point-of-failure ontstaat wat beperkend kan werken voor het kunnen bieden van dienstverlening en het uitvoeren van de organisatietaken. Indien een verwerking niet gelogd kan worden mag deze immers ook niet uitgevoerd worden.

Voordelen van een inrichting als magazijn is dat er via één punt gegevens ontsloten kunnen worden zonder dat er een single-point-of-failure ontstaat. Nadeel is dat de gegevens die ontsloten worden niet per definitie de meest actuele gegevens zijn.

Voor beide soorten van centrale inrichting geldt dat de ontsluiting van de loggegevens naar afnemers van die gegevens eenvoudig is doordat het aantal bronnen wat bevraagd moet worden gelimiteerd is.

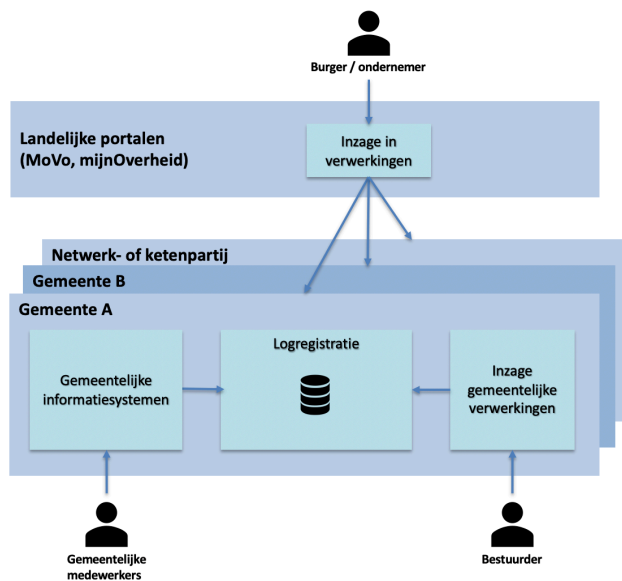
In onderstaande tabel worden de voor- en nadelen van de verschillende centrale inrichtingsscenario's opgesomt.

	Variant	Nadelen	Voordelen
Landelijk centraal	Bronregistratie	<ul style="list-style-type: none"> Potentieel <i>landelijk</i> single-point-of-failure Potentieel privacy hotspot Landelijke voorziening inclusief beheer organisatie vereist 	<ul style="list-style-type: none"> Gemeenten worden volledig ontzorgt Eenvoudige implementatie voor afnemende en aanleverende partijen door uniformiteit Centraal punt voor filtering Centraal punt voor ontsluiting loggegevens van de overheid Eenvoudige auditing op rechtmatigheid van verwerkingen
	Magazijn	<ul style="list-style-type: none"> Geen bevraging bij de bron, actualiteit gegevens loopt achter op de bron Synchronisatiemechanisme met bronnen nodig Potentieel privacy hotspot 	<ul style="list-style-type: none"> Gemeenten worden ten aanzien van ontsluiting van logging ontzorgt Centraal punt voor filtering

		<ul style="list-style-type: none"> Landelijke voorziening inclusief beheer organisatie vereist 	<ul style="list-style-type: none"> Centraal punt voor ontsluiting loggegevens van de overheid
Collectief centraal	Bronregistratie	<ul style="list-style-type: none"> Potentieel <i>collectief</i> single-point-of-failure Potentieel privacy hotspot Collectieve voorziening inclusief beheer organisatie vereist 	<ul style="list-style-type: none"> Altijd meest recente gegevens beschikbaar Individuele participerende gemeenten worden ontzorgd Centraal punt voor filtering Centraal punt voor ontsluiting gemeentelijke loggegevens van de overheid Eenvoudige auditing op rechtmatigheid van verwerkingen
	Magazijn	<ul style="list-style-type: none"> Geen bevraging bij de bron, actualiteit gegevens loopt achter op de bron Synchronisatiemechanisme met gemeentelijke bronnen nodig Potentieel privacy hotspot Collectieve voorziening inclusief beheer organisatie vereist 	<ul style="list-style-type: none"> Gemeenten worden ten aanzien van ontsluiting van loggegevens ontzorgd Centraal punt voor filtering Centraal punt voor ontsluiting gemeentelijke loggegevens van de overheid
Gemeentelijk lokaal	Bronregistratie	<ul style="list-style-type: none"> Potentieel <i>gemeentelijk</i> single-point-of-failure Potentieel privacy hotspot Gemeentelijke voorziening inclusief beheer vereist 	<ul style="list-style-type: none"> Altijd meest recente gegevens beschikbaar Lokale informatiesystemen worden ontzorgd Relatief eenvoudige ontsluiting van loggegevens naar afnemers Centraal punt voor filtering Eenvoudige auditing op rechtmatigheid van verwerkingen
	Magazijn	<ul style="list-style-type: none"> Geen bevraging bij de bron, actualiteit gegevens loopt achter op de bron Synchronisatiemechanisme met gemeentelijke bronnen nodig Potentieel privacy hotspot Gemeentelijke voorziening inclusief beheer vereist 	<ul style="list-style-type: none"> Relatief eenvoudige ontsluiting van loggegevens naar afnemers Centraal punt voor filtering

5.2. Gefedereerde inrichting

Bij een gefedereerde opslag van loggegevens worden loggegevens in meerdere logregistraties bijgehouden. Een gefedereerde inrichting kan zowel nationaal als lokaal worden geïmplementeerd. Bij een nationaal gefedereerde logregistratie is iedere overheidsorganisatie verplicht om zelf een logregistratie te voeren. De logregistraties van de verschillende organisaties kunnen in een gefedereerde inrichting wel vanuit een centraal punt ontsloten worden.

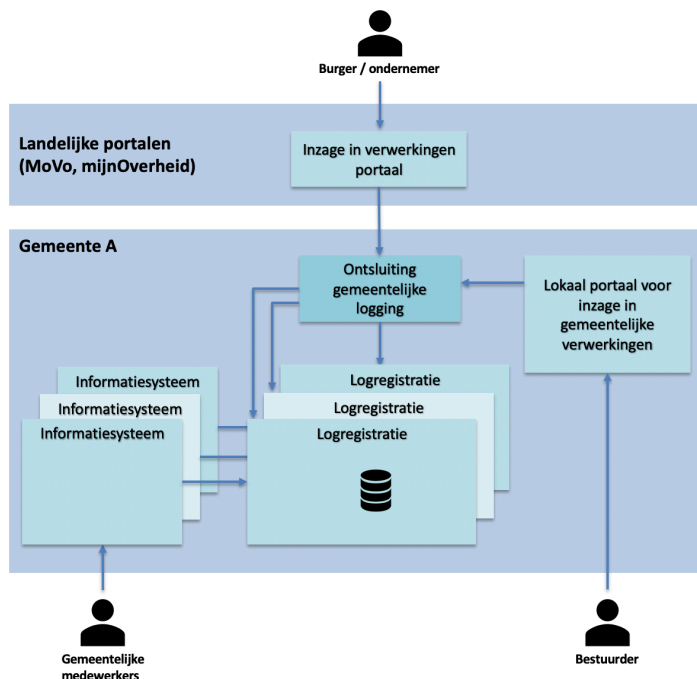


Figuur 11 – Landelijk gefedereerde logging inrichting

Iedere gemeente houdt in de landelijk gefedereerde inrichting een eigen logregistratie bij en ontsluit die naar geautoriseerde interne- en externe stakeholders. Een burger kan in dit model via verschillende toegangsvoorzieningen, zoals mij Overheid of andere portalen, de verwerkingen inzien die door gemeenten op zijn of haar persoonsgegevens zijn uitgevoerd. De toegangsvoorzieningen bevragen hiertoe alle gemeenten.

	Nadelen	Voordelen
Landelijk gefedereerd (logregistratie per organisatie)	<ul style="list-style-type: none"> ▪ Inzage geven in loggegevens is complex doordat meerdere bronnen bevroegd moeten worden ▪ Potentieel performance problematiek bij opvragen gegevens bij de verschillende bronnen ▪ Filtering van logging gegevens dient door iedere individuele organisatie uitgevoerd te worden 	<ul style="list-style-type: none"> ▪ Gegevens worden bijgehouden bij de bron; ▪ Opvragen van gegevens bij de bron en daardoor altijd actueel; ▪ Geen centraal privacy hotspot.

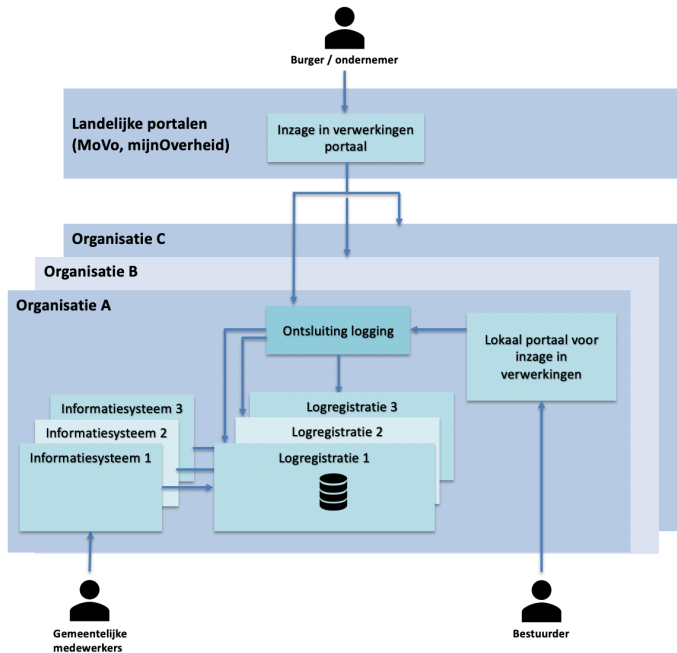
Naast een landelijk gefedereerde inrichting kan er ook sprake zijn van een lokale gefedereerde inrichting. In dit geval kent een organisatie geen centraal lokaal logregister maar ligt de verantwoordelijkheid van het vastleggen van logging bij informatiesystemen, of organisatorische afdelingen van de betreffende organisatie. De organisatie kent in dat geval een (groot) aantal logregistraties die allen een deel van de logging van verwerkingen binnen de organisatie bevatten.



Figuur 12 - Lokaal gefedereerde logging inrichting

Lokaal gefedereerd (meerdere lokale logregistraties)	<ul style="list-style-type: none"> Inzage geven in loggegevens is complex doordat meerdere bronnen bevraagd moeten worden Potentieel performance problematiek bij opvragen gegevens bij de verschillende bronnen Filtering van logging gegevens dient door iedere individuele lokale logregistratie uitgevoerd te worden Verskillende logregistraties nodig met bijbehorend beheer Complexe ontsluiting van gemeentelijke loggegevens als geheel Lokaal beheer van logregistraties 	<ul style="list-style-type: none"> Geen lokaal privacy hotspot; Gegevens worden gelezen uit de bronregistraties (de gegevensverwerkende systemen) en de gegevens zijn daarvoor altijd actueel
---	--	---

Een combinatie van een nationaal en lokaal gefedereerde inrichting levert een complexe omgeving op ten aanzien van de ontsluiting van logregisters. Organisaties zijn dan zelf verantwoordelijk voor de bijhouding van de logging van verwerkingen en doen dat via meerdere lokale logregistraties.



Een volledig overzicht van verwerkingen over alle organisaties heen in een landschap wat zowel nationaal als lokaal gefedereerd is opgebouwd kan alleen worden gevormd door alle bronnen van alle organisaties te bevrage, of door de inrichting van een centrale index waarin is aangegeven welke bronnen bevroegd moeten worden. Dat vraagt niet alleen om een centraal overzicht van te bevrage organisaties maar ook van de verschillende bronnen binnen een organisatie. Een organisatie dient richting het landelijk federatief stelsel logging te ontsluiten via een centraal punt. Indien een organisatie intern kiest voor een federatie van logregisters dan is die organisatie verplicht om een centrale dienst beschikbaar te stellen waarmee al de logregisters van die organisatie ontsloten worden.

6. Gemeentelijke inrichting

Vanuit wet- en regelgeving is iedere gegevensverwerkende organisatie zelf verantwoordelijk voor het loggen van de (metagegevens) van verwerkingen. Daarnaast wordt van organisaties geëist dat ze richting burger en ondernemer transparantie kunnen bieden over de verwerkingen. Zowel vanuit de centrale- als federatieve inrichting kan een organisatie invulling geven aan deze eisen. Wel zijn er tussen deze inrichtingen grote verschillen te onderkennen in complexiteit, kosten en flexibiliteit. De beweging van de overheid naar federatieve voorzieningen en de aan de privacy gerelateerde risico's van een centrale voorziening zijn belangrijke redenen om aan te kunnen nemen dat er, zeker op korte termijn, geen landelijk (basis)register voor loggegevens zal worden ingericht. Op landelijk niveau zal een gefedereerde inrichting ontstaan waarin iedere (overheids)organisatie zelf verwerkingen in logregisters zal vastleggen. Ook gemeenten hebben deze verantwoordelijkheid en zijn zelf verantwoordelijk voor het inrichten van een dergelijke voorziening. Gemeenten hebben de vrijheid om te kiezen uit de volgende mogelijkheden:

- Een centrale voorziening voor alle gemeenten;
- Een centrale binnengemeentelijke inrichting, of
- Een gefedereerde binnengemeentelijke inrichting.

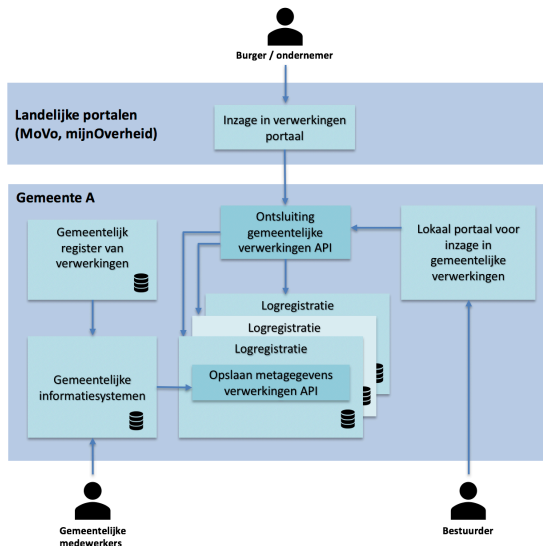
De voor- en nadelen van de verschillende inrichtingsvarianten zijn in voorgaande hoofdstukken beschreven.

De keuze voor een centrale voorziening voor alle gemeenten is niet zozeer een informatiekundige vraag, maar meer een vraag op het gebied van Samen Organiseren. Willen gemeenten allemaal lokaal de registratie van verwerkingen voeren of willen ze vanuit het oogpunt van kosten- en complexiteitsreductie één oplossing voor alle gemeenten. Deze vraag wordt vanuit dit document niet beantwoord maar is in de uiteindelijke totstandkoming van een oplossing wel van belang om te beantwoorden.

Doordat een landelijke voorziening voor logging niet te verwachten is, en landelijk er dus sprake is van een gefedereerd stelsel van logging worden gemeenten verplicht om de (metagegevens¹¹) van verwerkingen lokaal bij te houden. Vastlegging van de metagegevens van de verwerking van persoonsgegevens door gemeentelijke informatiesystemen is vanuit de AVG verplicht. In de metagegevens dienen onder meer de doelbinding en grondslag van de verwerking opgenomen te worden. Deze doelbinding en grondslag moeten gemeenten conform de AVG vastleggen in een 'gemeentelijk register van verwerkingen'. De eisen die aan de inrichting en het gebruik van dit register worden gesteld zijn beschreven in het document "GEMMA Gegevenslandschap - Register van verwerkingsactiviteiten".

De gemeente stelt conform verplichtingen vanuit de AVG de gegevens vanuit het lokale logregister, of de logregisters, beschikbaar aan geautoriseerde binnen- en buitengemeentelijke afnemers.

¹¹ <https://github.com/VNG-Realisatie/gemma-verwerkingen>



Figuur 13 - Inrichting opslag en ontsluiting gemeentelijk logregistratie

6.1. Opslag van loggegevens

Iedere organisatie is verplicht om metagegevens van verwerkingen van gegevens bij te houden en te ontsluiten. Het is mogelijk, en zelfs waarschijnlijk, dat een organisatie meerdere informatiesystemen gebruikt om invulling te geven aan de taken van die organisatie. Het is de verantwoordelijkheid van de organisatie om te borgen dat de verwerkingen van deze systemen gelogd worden en als geheel worden ontsloten. Ten aanzien van de opslag van de logging gelden de volgende spelregels:

- De logging betreft de metagegevens van verwerkingen zowel tussen gemeentelijke informatiesystemen als verwerkingen met buitengemeentelijke informatiesystemen van keten- en netwerkpartijen;
- Logging wordt gerelateerd aan een doelbinding en grondslag;
- Ieder informatiesysteem is verplicht verwerkingen van persoonsgegevens te loggen;
- Informatiesystemen kunnen optioneel ook de verwerking van overige objecten loggen;
- Bij een verwerking worden zowel de poging van de verwerking als het resultaat vastgelegd in de logging;
- Het logregister bevat alle relevante gegevens die nodig zijn voor het bieden van transparantie over verwerkingen. Er zijn geen andere bronnen nodig om deze transparantie te bieden;
- Bij de registratie van de logging wordt gebruikt gemaakt van het VNG-Realisatie logging informatiemodel¹²;
- Bij ieder logrecord wordt een unieke logidentificer bijgehouden waarmee logrecords van organisaties onderling aan elkaar gerelateerd kunnen worden. Het is de verantwoordelijkheid van de initieel vragende dienstenafnemer om een unieke logidentificer aan te leveren;

¹² <https://github.com/VNG-Realisatie/gemma-verwerkingen>

- Zowel aanvragend als gegevens leverend binnengemeentelijk informatie systeem loggen alle individuele verwerkingen van objecten. Dit houdt in dat in het geval dat een verzoek van een dienstenafnemer een resultaat oplevert wat meerdere objecten bevat zowel het leverende als het vragende systeem alle individuele records logt.
- Voor keten- en netwerkpartijen is het lastig om verplichtingen qua logging af te dwingen. Er wordt naar gestreefd om binnen koppelvlakken deze verplichtingen af te spreken met partijen ;
- Logbestanden zijn immutable (onaanpasbaar). Op geen enkele wijze mogen de logbestanden aangepast worden na het aanmaken van een logrecord. Zowel technisch als organisatorisch dienen organisaties maatregelen getroffen te worden om dit te borgen.
- Logging is direct raadpleegbaar door geautoriseerde binnen- en buitengemeentelijke afnemers;
- Als logging persoons en procesgegevens bevat valt deze onder de archieven van de gemeente
- Alle informatiesystemen die loggen gebruiken zelfde tijd(bron)

Het staat organisaties vrij om een centraal gemeentelijk logregister in te richten, of logregisters per informatiesysteem bij te houden. Randvoorwaarde is wel dat deze registraties via één API ontsloten moeten worden naar geautoriseerde raadplegers. De complexiteit van het intern voeren van meerdere logregisters en via een centraal punt ontsluiten van deze registers dient door de gemeente opgelost te worden. Ook moet het mogelijk zijn om de logregistratie te ontsluiten naar een SIEM¹³.

De API(s) voor de opslag van logging worden door VNG-Realisatie vastgesteld en zijn gebaseerd op het informatiemodel logging en de landelijke API en URI strategie.

6.2. Ontsluiting van logging

Iedere organisatie is verplicht om logging bij te houden en te ontsluiten. Ten aanzien van de ontsluiting van deze logging gelden de volgende spelregels:

- De logregistratie wordt door de gemeente via één gestandaardiseerde API ontsloten te worden naar afnemers.;
- Logging moet actief doorgegeven kunnen worden naar een SIEM oplossing;
- Indien logging intern in meerdere bronnen wordt opgeslagen is het de verantwoordelijkheid van de organisatie om deze verschillende bronnen als een samenhangende (virtuele) registratie te ontsluiten;
- Filtering van logginggegevens naar geautoriseerde afnemers is de verantwoordelijkheid van de gemeente;
- Bevraging van logging is alleen mogelijk door geautoriseerde organisaties;
- Bij het opvragen van de loggegevens wordt door de vragende partij aangegeven wat de doelbindingsclaim is voor de bevraging¹⁴;
- Bevraging van loggegevens wordt gelogd;
- Wijziging / vernietiging van loggegevens wordt gelogd

¹³ Specificaties hiervoor volgen nog. Zie <https://github.com/VNG-Realisatie/cg-architectuur/issues/57>

¹⁴ Het is aan te bevelen om de doelbindingsclaim voor het inzien van logging te standaardiseren over gemeenten heen. Op die manier is het eenvoudig om de acties in het kader van bijvoorbeeld regie op gegevens door de burger te scheiden van de logging van dienstverleningsprocessen.

Indien gegevens zijn uitgewisseld met een andere organisatie gelden aanvullende eisen:

- De gegevens die de logging inzage API teruggeeft bevat de naam van de organisatie waarmee gegevens zijn uitgewisseld;
- Aan de hand van de naam van een organisatie is het mogelijk zijn om de logging inzage API van die organisatie aan te roepen (URI strategie) zodat een keten van aanroepen geautomatiseerd kan worden bevraagd.

De API(s) voor de ontsluiting van logging worden door VNG Realisatie vastgesteld en zijn gebaseerd op het informatiemodel logging en de landelijke API en URI strategie. De API zal een aantal zoekingen ondersteunen. Zoekingangen die voor de hand liggen: objectidentificatienummer (bijvoorbeeld BSN), doelbinding, grondslag, datum/tijd

6.3. Filtering van loggegevens

Organisaties die loggegevens leveren dienen de afweging te maken of de burger (of andere eigenaar) in alle loggegevens inzicht mag krijgen. Met name verwerkingen vanuit bijvoorbeeld Sociale Inlichtingen- en Opsporingsdienst (SIOD) zullen veelal niet direct aan de burger getoond moeten worden aangezien dit de burger inzicht kan geven in lopende onderzoeken. Het permanent verbergen van loggegevens is echter niet de bedoeling. Zodra deze gegevens aan de burger mogen worden getoond, bijvoorbeeld na afloop van een fraudeonderzoek door een dienst, dienen de betreffende loggegevens vrijgegeven te worden naar de burger. Het is de verantwoordelijkheid van de organisatie die de beperking op de logrecords (en dus unieke logidentifiers) heeft geplaatst om deze loggegevens ook weer vrij te geven. Dit betekent dat delen van de logging geclassificeerd moeten worden op gevoeligheid, per proces en soort onderzoek.

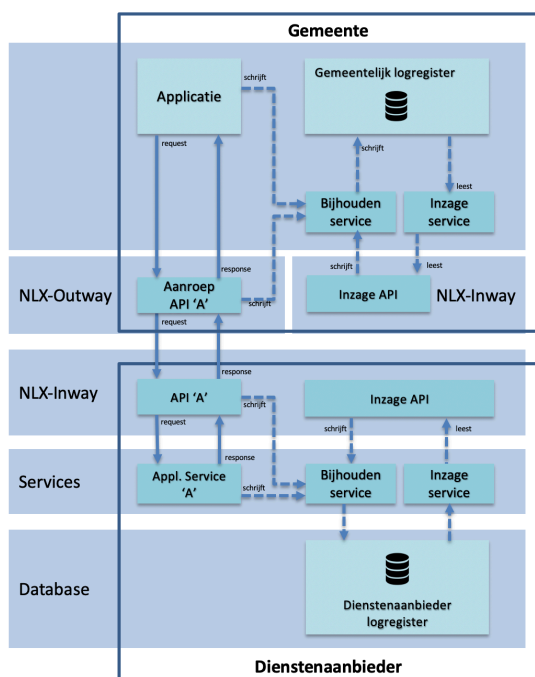
Partijen in de keten dienen de vrijgave van loggegevens in hun lokale registratie door te voeren en door te geven naar eventuele partijen met wie zij in de afhandeling van de verwerking hebben gecommuniceerd.

7. NLX implementatie logging

In dit hoofdstuk wordt beschreven hoe informatiesystemen die gebouwd zijn volgens het gemeentelijk gegevenslandschap en gebruik maken van NLX de gekozen federatieve inrichting van de logging van verwerkingen implementeren. Uitgangspunt hierbij is dat zowel de gemeente als de dienstenaanbieder waarmee gecommuniceerd wordt gebruik maakt van NLX voor de onderlinge connectiviteit.

7.1. Architectuur

Bij de gefedereerde opslag van logging gegevens worden logrecords lokaal vastgelegd door de individuele partijen tussen wie transacties worden uitgevoerd: de dienstenaanbieder en aanbieder. Bij deze partijen wordt logging bijgehouden door de NLX-node (inway of outway), de applicatie die een dienst gebruikt (dienstenaanbieder) en het informatiesysteem wat invulling geeft aan een API (dienstenaanbieder). Door de logregistraties van aanbieder en afnemers te combineren kan een logging audit trail worden gevormd. Vanuit deze logging trail wordt een beeld gegeven van de keten van organisaties die ten behoeve van een specifiek doel gegevens hebben verwerkt.



In bovenstaand figuur wordt weergegeven:

- Eén gemeente als afnemer van een dienst en een aanbieder van dienst 'A'. Zowel de gemeente als de dienstenaanbieder maken gebruik van NLX voor de onderlinge connectiviteit en beiden voeren een eigen logregister;

- De gemeente heeft een applicatie die gebruik maakt van de dienst 'A' van de dienstenaanbieder.
- De afnemer heeft een logregistratie die gevuld wordt vanuit de lokale NLX-outway en de applicatie die de externe API 'A' aanroept. De logregistratie van de gemeente wordt ontsloten via een logging inzage API die via een lokale NLX-inway ter beschikking wordt gesteld;
- De aanbieder biedt API 'A' aan afnemers via een NLX-inway. Deze API wordt gerealiseerd door 'Applicatie service A'. Het informatiesysteem wat deze applicatieservice aanbiedt is niet in het figuur opgenomen;
- De dienstenaanbieder voert een lokaal logregister dat gevuld wordt door de NLX-inway en de applicatieservice. Het logregister wordt ontsloten via een logging inzage API die aangeboden wordt via de lokale NLX-inway.

De logging inzage API van zowel de gemeente als dienstenaanbieder loggen de inzage verwerkingen. De logging inzage API leest en schrijft dus naar het lokale logregister.

7.2. Opslag loggegevens

Iedere organisatie die is aangesloten op NLX is verplicht om de audit logging bij te houden en te ontsluiten. Het gaat hierbij om de logging binnen de verwerkende informatiesystemen (zoals beschreven in het voorgaande hoofdstuk) en de logging binnen NLX. Het is de verantwoordelijkheid van de organisatie om te borgen dat de verwerkingen van de informatiesystemen en NLX-nodes gelogd worden en als geheel worden ontsloten. Ten aanzien van de opslag van de logging gelden de volgende spelregels aanvullend aan de in paragraaf 6.1 genoemde spelregels:

- De logging betreft zowel verwerkingen binnen de NLX-in en -outways als verwerkingen binnen gegevens afnemende en aanleverende informatiesystemen;
- Zowel *request* als *response* van een verzoek worden door NLX in- en outways vastgelegd in de logging.

De NLX-nodes hebben geen toegang tot de payload van berichten en hebben dus geen weet van welke objecten verwerkt worden. De NLX-nodes beperken zich tot de logging van metagegevens van API-aanroepen.

7.3. Ontsluiting van logging

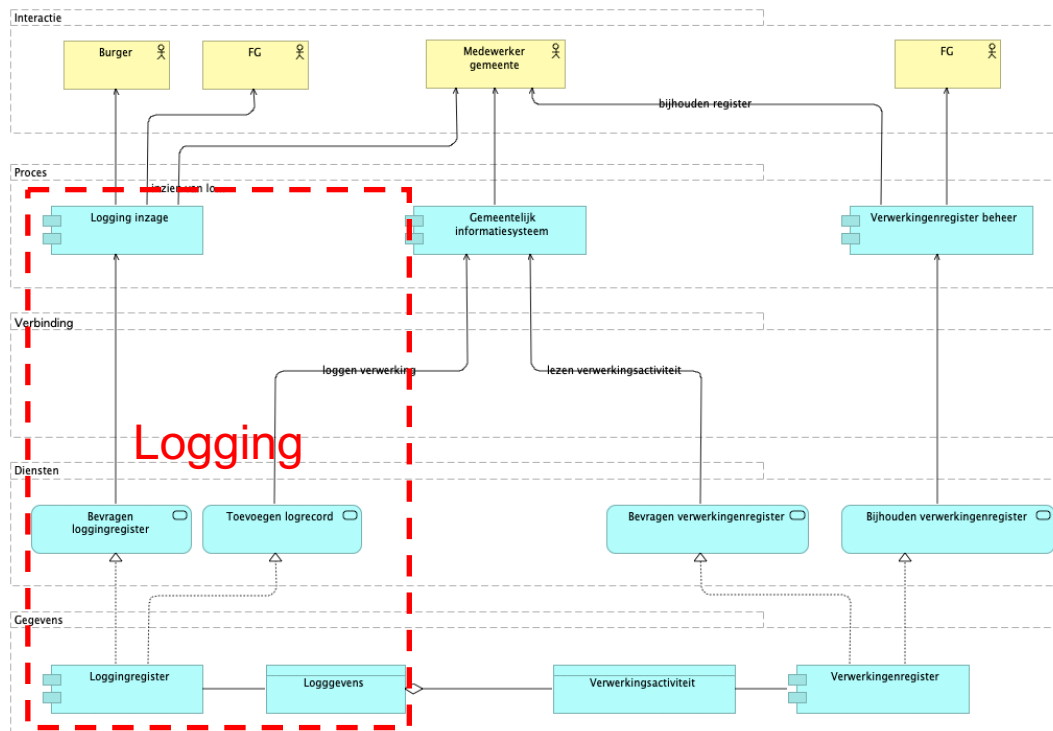
Iedere organisatie die is aangesloten op NLX is verplicht om logging bij te houden en te ontsluiten naar geautoriseerde afnemers. Ten aanzien van de opslag van de logging gelden de volgende spelregels aanvullend aan de in paragraaf 6.2 genoemde spelregels:

- Door de organisatie worden de loggevens ontsloten via een NLX-inway dienst.

Doordat logging binnen het NLX-netwerk gefedereerd wordt bijgehouden door de organisaties die zijn aangesloten is ontsluiting van de logging complex. Iedere partij in het NLX-netwerk kan immers potentieel loggegevens van een object (bijvoorbeeld een persoon) bijhouden. Om als burger een compleet beeld te krijgen van verwerkingen van persoonsgegevens door de overheid moet dus potentieel iedere individuele organisatie bevraagd worden.

8. GEMMA componenten

In de voorgaande hoofdstukken is beschreven dat gemeenten vanuit de AVG verplicht zijn om logging van verwerkingen bij te houden. Van de verwerkingen worden diverse metadata opgeslagen in een loggingregister. Onderdeel van de metadata zijn doelen en wettelijke grondslagen van. Het loggingregister wordt door VNG Realisatie breder gepositioneerd dan enkel voor de verwerkingen van persoonsgegevens. Dit register gaat ook verwerkingen van andere objecten bevatten.

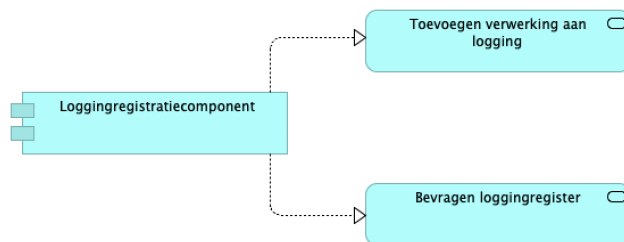


Figuur 14 - Samenhang componenten en actoren

In bovenstaand figuur is per laag van het architectuurmodel welke architectuurelementen een rol spelen bij de logging van verwerkingen.

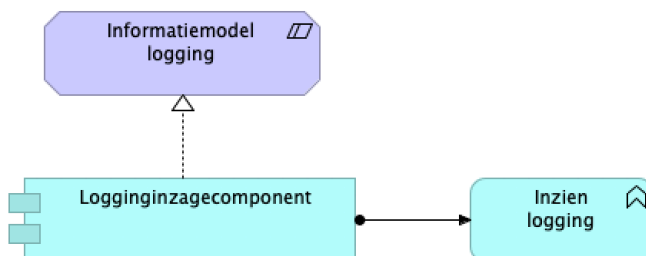
8.1. Loggingregister

Het loggingregister wordt gebruikt voor opslag en ontsluiting van loggingrecords. Het register ondersteunt de opslag van metagegevens die gerelateerd zijn aan een verwerking van gegevens conform het informatiemodel logging. De logginggegevens worden door gemeentelijke informatiesystemen aan de loggingregistratiecomponent aangeleverd via gestandaardiseerde APIs. Het loggingregister biedt daarnaast APIs voor het zoeken in de logging en het bevragen van de logging.



8.2. Logginginzagecomponent

De logginginzagecomponent is de component waarmee loggingrecords die in een loggingregister zijn opgeslagen kunnen worden ingezien. De logginggegevens worden ontsloten via de bevragings-APIs die door het loggingregister worden geboden.



Bijlage 1: Bronnen

- NL DIGIbeter: Agenda Digitale Overheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, juli 2018,
https://vng.nl/files/vng/bzk_brede_agenda_digitale_overheid_v12.pdf
- Nederlandse digitaliseringsstrategie, Overheid.nl
<https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/nederlandse-digitaliseringsstrategie>
- Onderzoeksrapport Waardevol digitaliseren, Rathenau Instituut, juni 2018
https://vng.nl/files/vng/rapport-rathenau_instituut_waardevol_digitaliseren.pdf
- Aanwijzing logging, Gemeentelijke Informatiebeveiligingsdienst, januari 2014
<https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2014/04/14-0106-Aanwijzing-Logging.pdf>
- Checklist Data Privacy Impact Analyse, Gemeentelijke Informatiebeveiligingsdienst, augustus 2018,
<https://www.informatiebeveiligingsdienst.nl/nieuws/checklist-data-privacy-impact-analyse/>